

Abstract of Disclosure

A transmission apparatus performs a one-way operation on the plaintext to generate a first value and transmits the first value, generates first additional information, performs an invertible operation on the plaintext and the first additional information to generate connected information, encrypts the connected information according to an encryption algorithm to generate ciphertext, and transmits the ciphertext.

A reception apparatus receives the first value and the ciphertext, generates a second additional information which is identical to the first additional information, decrypts the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm to generate decrypted connected information, decrypts the decrypted connected information and the second additional information according to an inverse operation of the invertible operation to generate decrypted text, performs the one-way operation on the decrypted text to generate second value, compares the first and the second values, and judges that the decrypted text is valid only when the first and the second values match.